Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 20 (1974)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $y^2 \equiv x^4 – a(mod \quad p)$

Autor: Singh, Surjit / Rajwade, A. R.

DOI: https://doi.org/10.5169/seals-46910

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 13.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $y^2 \equiv x^4 - a \pmod{p}$

by Surjit SINGH and A. R. RAJWADE

1. INTRODUCTION

The object of this paper is to prove the following theorem.

THEOREM. *Let a be an integer not divisible by a given prime p. Then the number of solutions of the congruence $y^2 \equiv x^4 - a \pmod{p}$ is*

$$\begin{cases} p - 1 \ \ if \ \ p \equiv 3 \pmod{4}. \\ p - (a/\pi)_4 \bar{\pi} - (a/\bar{\pi})_4 \pi - 1 \ \ if \ \ p \equiv 1 \pmod{4}. \end{cases}$$

where $(\frac{\cdot\cdot}{\cdot\cdot})_4$ is the biquadratic residue symbol and $p = \pi \bar{\pi}$ is the factorization of p in the ring $Z[i]$ of the Gaussian integers, π and $\bar{\pi}$ being both normalized $\equiv 1 \pmod{(2(1+i))}$.

Morlaye shows (see [4] Proposition 1) that if N is the number of solutions of the congruence $y^2 \equiv x^3 - ax \pmod{p}$ and N' the number of solution of the congruence $y^2 \equiv x^4 - a \pmod{p}$ then $N = N' + 1$. This is a short proposition for the case $p \equiv 1\ (4)$ and so our theorem gets the number of solutions of

$$y^2 \equiv x^3 - ax \pmod{p}$$

by yet another elementary method. This latter equation: $y^2 = x^3 - ax$ is the elliptic curve with complex multiplication by $\sqrt{-1}$. (See also a remark by Swinnerton-Dyer in [1]). A proof of the latter result is also given in [2] and [5]. These proofs, however, are not elementary.

We note here that both N and N' can be computed trivially for the case $p \equiv 3\ (4)$.

To get N we proceed as follows:

Case 1. a is a quadratic non-residue mod p. Then corresponding to $y = 0$, there exist only one x viz $x = 0$ satisfying

$$y^2 \equiv x(x^2 - a) \pmod{p}$$

since $x^2 - a \equiv 0\,(p)$ is not solvable. This gives one solution (0, 0). Let now $x = \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, be a complete non-zero residue system mod p. Of $x^3 - ax$ and $(-x)^3 - a(-x) = -(x^3 - ax)$ one is a quadratic residue and the other a non-residue since -1 is a non-residue, p being $\equiv 3\,(4)$. Hence as x takes the values $\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, $x^3 - ax$ becomes a quadratic residue $\frac{p-1}{2}$ times (perhaps with repetitions) and a non-residue $\frac{p-1}{2}$ times. Each time it is a quadratic residue, we get 2 solutions. Hence there exist $p - 1$ solutions, and together with (0, 0) gives p solutions as required.

Case 2. a is a quadratic residue mod p, that is there exists an x_0 such that $x_0^2 \equiv a \pmod{p}$. Then corresponding to $y = 0$ there exist 3 solutions, $(0, 0)$, $(x_0, 0)$, $(-x_0, 0)$. Let now $x = \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$, but $\neq \pm x_0$ (or 0) (all together $p - 3$ values). As above $x^3 - ax$ becomes a quadratic residue exactly $\frac{p-3}{2}$ times and so there exists $p - 3$ solutions, which together with $(0, 0)$, $(\pm x_0, 0)$ gives p solutions as required. To get N' we note that in this case the biquadratic residues of p are the same as quadratic residues. Hence the congruence can be written as

$$y^2 \equiv x^2 - a \pmod{p}$$

or

$$(x+y)(x-y) \equiv a \pmod{p}$$

or

$$u.v \equiv a \pmod{p}$$

which has $p - 1$ solutions as required. For the case $p \equiv 1 \pmod{4}$ we shall use results from cyclotomy for the factorization $p - 1 = 4f$.

2. The congruence $y^2 \equiv (x^4 - a) \pmod{p}$

Let $\left(\frac{t}{p}\right)$ be the Legendre symbol. The number of solutions of $y^2 \equiv x^4 - a \pmod{p}$ equals $\sum_x \left[1 + \left(\frac{x^4 - a}{p}\right)\right] = p + \sum_x \left(\frac{x^4 - a}{p}\right) = p + S$. To get S we define first the biquadratic character χ as follows:

Let g be a primitive root mod p. Then for any integer $m\ (\neq 0)$ there exists a positive integer v such that $m \equiv g^v\ (p)$. We put $\chi(m) = (i)^v$ where $i = \sqrt{-1}$ and put $\chi(0) = 0$. This defines χ. We now have

$$S = \sum_y [1 + \chi(y) + \chi^2(y) + \chi^3(y)] \left(\frac{y-a}{p}\right)$$
$$= \sum_y \chi(y) \left(\frac{y-a}{p}\right) + \sum_y \chi^2(y) \left(\frac{y-a}{p}\right) + \sum_y \chi^3(y) \left(\frac{y-a}{p}\right).$$

Setting $y = -az$ we get:

$$S = \left(\frac{-a}{p}\right) \left[\sum_{all\, z} \chi(-a)\chi(z) \left(\frac{z+1}{p}\right) + \sum_{all\, z} \chi^2(-a)\chi^2(z) \left(\frac{z+1}{p}\right) + \sum_{all\, z} \overline{\chi(-a)}\,\overline{\chi(z)} \left(\frac{z+1}{p}\right)\right],$$

since $\chi^3(m) = \overline{\chi(m)}$ for all integers m.
Now we look at the sum

$$\sum \chi(z) \left(\frac{z+1}{p}\right).$$

This equals

$$\sum_{z+1\, =\, square} \chi(z) - \sum_{z+1\, =\, not\ square} \chi(z).$$

But

$$0 = \sum_{z+1\, =\, square} \chi(z) + \sum_{z+1\, \neq\, square} \chi(z) + \chi(-1).$$

Therefore

$$\sum_{z+1\, =\, square\ not\ zero} \chi(z) = \tfrac{1}{2} \sum_{u \neq o} \chi(u^2 - 1) = \tfrac{1}{2} \sum_{u \neq o} \chi(u+1)\chi(u-1)$$
$$= \tfrac{1}{2} \Big[\sum_{all\, u} \chi(u+1)\chi(u-1) - \chi(-1)\Big].$$

Now put $u = 2v + 1$.
Therefore $\displaystyle\sum_{z+1\, =\, square\ not\ zero} \chi(z) = \tfrac{1}{2} \Big[\chi(4) \sum_{all\, v} \chi(v)\chi(v+1) - \chi(-1)\Big].$

Hence $\displaystyle\sum_{all\, z} \chi(z) \left(\frac{z+1}{p}\right) = \chi(4) \sum_{all\, v} \chi(v)\chi(v+1).$

Similarly for χ^2 and $\bar{\chi}$ and therefore we get

$$S = \left(\frac{-a}{p}\right) \Big[\chi(-4a) \sum_{all\, v} \chi(v)\chi(v+1) + \bar{\chi}(-4a) \sum_{all\, v} \bar{\chi}(v)\bar{\chi}(v+1) + \chi^2(-4a) \sum_{all\, v} \chi^2(v)\chi^2(v+1)\Big].$$

3. Cyc otomy for $p = 1 + 4f$.

Let g be a primitive root mod p which we have already fixed in § 2. Divide the non-zero residues mod p into four classes A_0, A_1, A_2, A_3 by putting $m \equiv g^v$ in A_i if $v \equiv i \pmod 4$. The cyclomic constants (h, k) $(0 \leqslant h, k \leqslant 3)$ are defined to be the number of values of y, $1 \leqslant y \leqslant p - 2$ for which

$$(3.1) \qquad y \equiv g^{4t+h} \pmod p, \qquad 1 + y \equiv g^{4s+k} \pmod p$$

[i.e. for which $y \in A_h$, $1 + y \in A_k$].

As results differ in the two cases $p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$ we look as these cases separately.

Case 1 : $p \equiv 1 \pmod 8$. In this case $p = 1 + 4f$ where f is even. We know [3] that

$$(3.2) \qquad \begin{cases} (h, k) = (k, h) \\ (h, k) = (-h, k-h) \end{cases}$$

Thus $(1, 2) = (2, 3) = (1, 3)$; $(1, 1) = (0, 3)$; $(2, 2) = (0, 2)$; $(3, 3) = (0, 1)$. Therefore of the 16 cyclotomic constants which may be written as a (4×4) matrix, only five are different and we have

$$(3.3) \qquad \begin{bmatrix} (0,0) & (1,0) & (2,0) & (3,0) \\ (0,1) & (1,1) & (2,1) & (3,1) \\ (0,2) & (1,2) & (2,2) & (3,2) \\ (0,3) & (1,3) & (2,3) & (3,3) \end{bmatrix} = \begin{bmatrix} A & D & C & B \\ D & B & E & E \\ C & E & C & E \\ B & E & E & D \end{bmatrix}$$

Consider the numbers $1, 2, \ldots, p - 1$. Each $y \in A_0$ (there are f such y's) except the last (i.e. $p - 1$ which is in A_0 in this case) is followed by $y + 1$ which may belong to A_0, A_1, A_2 or A_3.

Similarly each $y \in A_1$ without exception is followed by $y + 1$ which may belong to A_0, A_1, A_2 or A_3 and so on. Hence we get

$$(3.4) \qquad A + D + C + B = f - 1$$

$$(3.5) \qquad D + B + 2E = f$$

$$(3.6) \qquad 2C + 2E = f.$$

Case 2: $p \equiv 5 \pmod 8$. In this case $p = 4f + 1$ where f is odd. Now look at the congruence

$$1 + g^{4t+h} + g^{4s+k} \equiv 0 \pmod p. \tag{3.1$'$}$$

Denote the number of solutions of (3.1)′ by $\{h, k\}$. Then clearly $\{h, k\} = \{k, h\}$ and the following relations are known [3]

$$\begin{cases} \{-h, k-h\} = \{h, k\} \text{ for any } f \text{ even or odd} \\ \{h, k\} \qquad\qquad = (h, k+2) \text{ for } f \text{ odd.} \end{cases} \tag{3.2$'$}$$

Thus $\{1, 0\} = \{3, 3\}$; $\{3, 0\} = \{1, 1\}$; $\{2, 0\} = \{2, 2\}$ and $\{3, 1\} = \{1, 2\} = \{3, 2\}$.

Therefore the matrix of the cyclotomic constants $\{h, k\}$ can be written as

$$\begin{bmatrix} \{0,0\} & \{1,0\} & \{2,0\} & \{3,0\} \\ \{0,1\} & \{1,1\} & \{2,1\} & \{3,1\} \\ \{0,2\} & \{1,2\} & \{2,2\} & \{3,2\} \\ \{0,3\} & \{1,3\} & \{2,3\} & \{3,3\} \end{bmatrix} = \begin{bmatrix} L & M & N & R \\ M & R & S & S \\ N & S & N & S \\ R & S & S & M \end{bmatrix} \tag{3.3$'$}$$

Since f is odd, $p - 1$ belongs to A_2 hence in this case as before

$$(0, 1) + (0, 1) + (0, 2) + (0, 3) = f$$
$$(1, 0) + (1, 1) + (1, 2) + (1, 3) = f$$
$$(2, 0) + (2, 1) + (2, 2) + (2, 3) = f - 1 .$$

Now using (3.2)′ and (3.3)′ we get

$$L + M + N + R = f \tag{3.4$'$}$$
$$R + M + 2S = f \tag{3.5$'$}$$
$$2N + 2S = f - 1 . \tag{3.6$'$}$$

4. The Jacobi function

Let α be any root ($\neq 1$) of $\alpha^{p-1} = 1$. Write

$$F(\alpha) = \sum_{k=o}^{p-2} \alpha^k \zeta^{q^k} \text{ where } \zeta^p = 1 \text{ and } \zeta \neq 1 . \tag{4.1}$$

We shall employ a special case of the function (4.1) due to Jacobi. Let $p = ef + 1$ and β be a primitive e-th root of unity. In (4.1) take $\alpha = \beta^n$ (n-integer). We know ([3] page 395) that if e does not divide n then

$$F(\beta^n) F(\beta^{-n}) = (-1)^{nf} \cdot p \tag{4.2}$$

and if we put

$$R(n, m) = \frac{F(\beta^n) F(\beta^m)}{F(\beta^{m+n})}, \tag{4.3}$$

then

$$R(n, m) = \sum_{h=0}^{e-1} \beta^{nh} \sum_{k=0}^{e-1} \beta^{-(m+n)k} (h, k). \tag{4.4}$$

From (4.2) and (4.3) it follows that if e does not divide m, n and $m + n$ then

$$R(n, m)\, R(-n, -m) = p \tag{4.5}$$

and from (4.4) it follows that $R(-n, -m)$ is got from $R(n, m)$ by replacing β by β^{-1}. Let now $e = 4$ and $\beta = \sqrt{-1}$; using (4.4) we get

$$R(1, 1) = (A - B - C - D + 2E) + i(2D - 2B) \text{ in case } p \equiv 1 \pmod 8$$
$$R(1, 1) = (L - M - R - N + 2S) + i(2M - 2R) \text{ in case } p \equiv 5 \pmod 8.$$

5. Proof completed

If $p \equiv 1 \pmod 4$ then p splits in $Z[i]$ as $p = \pi\bar{\pi}$ where π is prime in $Z[i]$.

Case 1 : $p \equiv 1 \pmod 8$.

$$\sum_{\text{all } v} \chi(v)\chi(v+1) = \sum_{v \in A_0, A_1, A_2, A_3} \chi(v)\chi(v+1) = \sum_{A_0} + \sum_{A_1} + \sum_{A_2} + \sum_{A_3}$$
$$= 1[A + Di - C - Bi] + i[D + Bi - E - Ei]$$
$$- 1[C + Ei - C - Ei] - i[B + Ei - E - Di]$$
$$= [A - B - C - D + 2E] + i[2D - 2B]$$
$$= R(1, 1) = (-2f + 8(1, 2) - 1) - 2i[D - B] \tag{5.1}$$

where $R(1, 1) \equiv -1 \pmod{2(1+i)}$ (as $D - B = f - 2B - 2E$ by (3.5))

and
$$\sum_{\text{all } v} \chi^2(v)\chi^2(v+1) = (A - D + C - B) - (D - B + E - E)$$
$$+ (C - E + C - E) - (B - E + E - D)$$
$$= A + 3C - D - 2E - B = -1,$$

by (3.4)

Therefore we have

$$S = \left(\frac{-a}{p}\right)\left[\chi(-4a)\,R(1,1) + \bar{\chi}(-4a)\,\overline{R(1,1)} + \chi^2(-4a)(-1)\right].$$

We put $\pi = -R(1,1)$, then $\pi \equiv +1 \pmod{2\,(1+i)}$.

Therefore $S = \left(\frac{-a}{p}\right)\left[-\chi(-4a)\,\pi - \bar{\chi}(-4a)\,\bar{\pi} - \chi^2(-4a)\right]$.

Let g be the primitive root mod p which we have already fixed in § 2. We now have two possibilities:

(i) $\left(\frac{g}{\pi}\right)_4 = i$ i.e. $\left(\frac{d}{\pi}\right)_4 = \chi(d)$ for all d.

(ii) $\left(\frac{g}{\pi}\right)_4 = -i$ i.e. $\left(\frac{d}{\pi}\right)_4 = \bar{\chi}(d)$ for all d.

Let $\chi(d) = \left(\frac{d}{\pi^*}\right)_4$ where $\pi^* = \pi$ or $\bar{\pi}$.

We shall show that $\pi^* = \pi$. We have

$$\pi = -\sum \chi(v)\,\chi(v+1) \equiv -\sum_{0}^{p-1} v^{\frac{1}{4}(p-1)}(v+1)^{\frac{1}{4}(p-1)} \bmod \pi^*$$

$$\equiv -\left[v^{\frac{1}{4}(p-1)}\left(1+\tfrac{1}{4}(p-1)v + \ldots + v^{\frac{1}{4}(p-1)}\right)\right] \bmod \pi^*.$$

In the last sum each term is divisible by $p = \pi\bar{\pi}$, because we know that $\sum_v v^k \equiv 0 \bmod p$ unless $p - 1/k$. Hence the right hand side of the above is congruent to zero mod π^*. Hence $\pi \equiv 0 \bmod \pi^*$ giving $\pi = \pi^*$.

Therefore

$$S = -\left(\frac{-a}{p}\right)\left(\frac{-4a}{\pi}\right)_4 \pi - \left(\frac{-a}{p}\right)\left(\frac{-4a}{\bar{\pi}}\right)_4 \bar{\pi} - \left(\frac{-a}{p}\right)\left(\frac{-4a}{\pi}\right)_4^2$$

$$= -\left(\frac{-4a}{\pi}\right)_4^3 \pi - \left(\frac{-4a}{\bar{\pi}}\right)_4^3 \bar{\pi} - 1 = -\left(\frac{a}{\pi}\right)_4^3 \pi - \left(\frac{a}{\bar{\pi}}\right)_4^3 \bar{\pi} - 1$$

$$= -\left(\frac{a}{\bar{\pi}}\right)_4 \pi - \left(\frac{a}{\pi}\right)_4 \bar{\pi} - 1,$$

using (i) $\left(\frac{d}{p}\right) = \left(\frac{d}{\pi}\right)_4^2 = \left(\frac{d}{\bar{\pi}}\right)_4^2$

(ii) $\left(\frac{d}{\pi}\right)_4^3 = \left(\frac{d}{\bar{\pi}}\right)_4$

(iii) $\left(\frac{-4}{\pi}\right)_4 = \left(\frac{-4}{\bar{\pi}}\right)_4 = 1$ since $-4 = (1+i)^4 -$ a fourth power.

This gives the required value of S.

Case 2 : $p \equiv 5 \pmod 8$. In this case as before

$$\sum \chi(v)\chi(v+1) = [N - L + R + M - 2S] + i[2R - 2M]$$
$$= -R(1,1) \text{ (see [3])}$$

and $\sum \chi^2(v)\chi^2(v+1) = 3N + L - 2S - R - M = -1$,
using (3.4)′, (3.5)′, (3.6)′, and therefore

$$S = \left(\frac{-a}{p}\right)[-\chi(-4a)R(1,1) - \bar{\chi}(-4a)\overline{R(1,1)} - 1 \,.\, \chi^2(-4a)] \,.$$

Here $R(1,1) = (L-M-R-N+2S) + i(2M-2R)$
$= (-2f+8(1,0)+1) + i(2M-2R)$ (see [3]) .

We put $R(1,1) = \pi$, then $\pi \equiv 1 \pmod{(2+2i)}$ and we get

$$S = \left(\frac{-a}{p}\right)[-\chi(-4a)\pi - \bar{\chi}(-4a)\bar{\pi} - \chi^2(-4a)]$$

and as before this

$$= -\left(\frac{a}{\bar{\pi}}\right)_4 \pi - \left(\frac{a}{\pi}\right)_4 \bar{\pi} - 1 \,,$$

as required. This completes the proof of the Theorem.

REFERENCES

[1] CASSELS, J. W. S. and A. FROHLICH. *Algebraic Number Theory*. Academic Press (1967), p. 284.

[2] DAVENPORT, H. and H. HASSE. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen. *J. reine angew. Math. 172* (1934), pp. 151-182.

[3] DICKSON, L. E. Cyclotomy, higher congurence and Waring's problems. *Am. J. Math, 57* (1935), pp. 391-423.

[4] MORLAYE, B. (1972). Démonstration élémentaire d'un théorème de Davenport et Hasse. *L'Enseignement mathématique 8*. (1972), pp. 269-276.

[5] RAJWADE, A. R. A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - D\,x \pmod{p}$. *Proc. Cambridge Phil. Soc. 67* (1970), pp. 603-605.

(Reçu le 20 novembre 1974)

Surjit Singh
A. R. Rajwade

Department of Mathematics
Panjab University
Chandigarh (India)

vide-leer-empty